



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

AAS:MAA
F. #2021R00963

*271 Cadman Plaza East
Brooklyn, New York 11201*

November 15, 2022

By ECF

The Honorable Eric R. Komitee
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Kambiz Attar Kashani
Criminal Docket No. 22-33 (EK)

Dear Judge Komitee:

The government respectfully submits this letter to supplement its October 25, 2022 sentencing memorandum (the “Sentencing Memorandum”) and in response to the Court’s direction during the defendant’s November 1, 2022 sentencing hearing (the “Sentencing Hearing”) that the government provide certain additional information. (See Tr. 29:20-32:4.) Specifically, the government below provides additional information regarding: (1) the business operations of UAE Company 1 and UAE Company 2; (2) the U.S. technology and goods the defendant and his co-conspirators illegally transshipped to Iran; (3) the effects of the illegal transshipping scheme; and (4) the reasons the government has not sought forfeiture of the defendant’s interests in UAE Company 1 and UAE Company 2.¹

I. UAE Company 1 and UAE Company 2

For the reasons below, the government respectfully submits that, during the period of the charged conspiracy, UAE Company 1 and UAE Company 2 functioned primarily, if not solely, to illegally transship goods and technology from U.S. companies to end users in Iran, including the Government of Iran. The government further submits that UAE Company 1 and UAE Company 2 are no longer operational.

Following the Sentencing Hearing, the government conferred with defense counsel regarding these matters.

¹ Capitalized terms not otherwise defined herein have the meanings ascribed in the Sentencing Memorandum.

A. UAE Company 1

i. Business Operations

During the Sentencing Hearing, defense counsel disputed that UAE Company 1 was “engaged in the sole purpose of illegally providing goods and services,” contending that it is an “accredited S[WIFT] Bureau” and listed on the SWIFT website. (See Tr. 14:8-12.) Defense counsel further contended that UAE Company 1 was certified by SWIFT and had agreements with certain Iranian banks and, at an unspecified time, two Iraqi banks, seeking to use SWIFT messaging services. (See *id.* 17:22-18:2.) For the reasons below, the government respectfully submits that, even to the extent UAE Company 1 conducted legal business as a SWIFT bureau – which is far from clear to the government, as set forth in footnote 2 – the defendant’s own involvement in providing SWIFT services to Iranian banks violated ITSR and U.S. sanctions. The government further submits that the business UAE Company 1 conducted as a SWIFT bureau – whether legal or not – constituted only a minor part of UAE Company 1’s business, with the vast majority of its business comprised of its indisputably illegal transshipping scheme.

As set forth in Exhibit A, the parties have stipulated that UAE Company 1 was established and structured in the UAE in or around 2011, at the direction of and with capital from Iran Company 1, to provide SWIFT services to Iranian banks. (See Plea Agreement, Ex. A ¶ 14.) The parties also stipulated that UAE Company 1 is a certified SWIFT service bureau, and as such has provided SWIFT services to Iranian and Iraqi banks pursuant to written agreements with them, and is subject to annual inspections by and certifications to SWIFT. (See *id.* ¶ 3.) The parties moreover have stipulated that, as UAE Company 1’s technical manager, the defendant was responsible for all technical issues relating to the SWIFT data centers and provision of SWIFT services, and that the defendant also was SWIFT’s contact person at UAE Company 1. (See *id.* ¶ 6.)

The defendant’s involvement in providing SWIFT services to Iranian banks violated ITSR and U.S. sanctions. As set forth in the Sentencing Memorandum, the U.S. Department of the Treasury, through OFAC, promulgated the ITSR. (See Dkt No. 31 at 2 (citing 31 C.F.R. Part 560).) The ITSR prohibits, among other things, the unlicensed export, re-export, sale or supply, directly or indirectly, from the United States or by a United States person, of any goods, services or technology to Iran or to the Government of Iran. (See *id.* (citing 31 C.F.R. Part 560).) The regulations also prohibit conspiring to and attempting to evade, avoid, or violate the regulations. (See *id.* (citing 31 C.F.R. Part 560).) The defendant, as a U.S. citizen, is prohibited (absent certain exceptions, which do not apply here) from exporting services – such as SWIFT services – to individuals and entities in Iran, no matter where he is located or whether he provides the services directly or indirectly. See 31 C.F.R. § 560.204(a) (“[T]he exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran is prohibited, including the exportation, reexportation, sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that . . . Such goods, technology, or services are intended specifically for supply, transshipment, or reexportation, directly or indirectly, to Iran or the Government of Iran[.]”); 31 C.F.R. § 560.208 (“[N]o United States person, wherever located, may approve, finance, facilitate, or guarantee any

transaction by a foreign person where the transaction by that foreign person would be prohibited by this part if performed by a United States person or within the United States.”). More broadly, OFAC has advised law enforcement that SWIFT cannot be operated out of Iran and that Iranian banks cannot utilize the SWIFT system. Further, law enforcement determined, based on review of the SWIFT website, that there are no SWIFT bureaus operating out of Iran.

In any event, based on law enforcement’s review, pursuant to judicially-authorized search warrants, of UAE Company 1’s emails from approximately 2019 through 2021, law enforcement determined that the vast majority of UAE Company 1’s activities during that period involved helping Iran Company 1 illegally obtain U.S.-origin goods and technology through transshipping schemes. Specifically, the majority of these emails related to business and transactions (i.e., purchases of U.S. goods and technology, in violation of U.S. sanctions) between UAE Company 1, UAE Company 2, Iran Company 1, and CBI. In contrast, a small percentage of the emails law enforcement reviewed reflected that UAE Company 1 operated as a SWIFT service bureau for Iranian banks and that UAE Company 1 managed data centers in the UAE and Turkey that maintained Iranian data. It is not clear that UAE Company 1’s SWIFT activities were legal,²

² SWIFT’s terms and conditions appear to prohibit business with Iran. SWIFT’s legal and financial criteria during at least part of the period of the charged conspiracy provide that: “The service bureau, its staff, and any associated agents must not be identified on any [European Union (“EU”)] and/or US sanctions lists and must not be registered in, or citizens of, any country targeted under EU and/or US Sanctions programs, which would restrict the provision of the intended services.” See SWIFT, Shared Infrastructure Programme: Terms and Conditions 2021, at 6 (Dec. 31, 2020), available at https://www2.swift.com/knowledgecentre/rest/v1/publications/shr_infra_prog_trm_cond_2021/2.0/shr_infra_prog_trm_cond_2021.pdf?logDownload=true. As set forth in Exhibit A, UAE Company 1 was established at the direction of and with capital from Iran Company 1, and Iran Company 1 and employees in Iran provided ongoing direction to UAE Company 1, including to the defendant. (See Plea Agreement, Ex. A ¶¶ 3, 8, 9.) Accordingly, at a minimum, UAE Company 1 appears to have violated SWIFT’s requirement that associated agents of UAE Company 1 must not be registered in a country targeted under U.S. (or EU) sanctions programs which would restrict provision of the intended services. Specifically, during the period of the charged conspiracy, Iran Company 1, registered in Iran, was an associated agent of UAE Company 1 and was targeted under U.S. (and EU) sanctions. The government notes that the parties also have stipulated that UAE Company 1 provided SWIFT services to Iraqi banks; it is not clear whether UAE Company 1 did so during the period of the charged conspiracy. Nevertheless, certain Iraqi entities were subject to U.S. sanctions, though the government has not been able to determine whether the Iraqi banks to which UAE Company 1 provided SWIFT services were sanctioned entities during the relevant time period. Moreover, according to defense counsel, UAE Company 1 at some point provided SWIFT services to two Iraqi banks (see Tr. 18:1-2), which clearly is a minimal portion of UAE Company 1’s business.

In addition, most Iranian banks were sanctioned under U.S. and/or EU law during the period of the charged conspiracy. Any SWIFT transactions involving those banks would not have been legal, given that SWIFT follows EU law and U.S. sanctions law. However, the government has not been able to determine the specific Iranian banks involved in UAE Company 1’s SWIFT transactions, nor whether they were sanctioned entities.

but even assuming, arguendo, that they were, such activities comprised only a minor part of UAE Company 1's business operations. Rather, the primary activity of UAE Company 1 was to illegally facilitate the transshipment of U.S. goods and technology to Iran Company 1, and at times, CBI.

ii. Current Status

The government's understanding is that – notwithstanding defense counsel's representations during the Sentencing Hearing (see Tr. 27:19-20) – UAE Company 1 is no longer operational.

First, in November 2022, the U.S. Department of Commerce ("Commerce") conducted an "end use check" to verify whether UAE Company 1 is still operational. As part of the end use check, Commerce reviewed the UAE Ministry of Economy's National Economic Register website, which maintains information about UAE business licenses and activity. Commerce was unable to locate a commercial business license for UAE Company 1 – which previously had a commercial license available on the website – thereby indicating that UAE Company 1 currently is not authorized to conduct business in the UAE.

Second, UAE Company 1's email domain – which is the email domain the defendant used to access SWIFT, as well as in furtherance of the illegal transshipping scheme – is no longer active. The U.S. service provider for UAE Company 1's email domain during the period of the charged conspiracy has confirmed to law enforcement that the domain is no longer registered or maintained by that provider. Similarly, UAE Company 1's website appears to have been disabled.

Third, recorded jail conversations between the defendant, his son, and his wife – including a call occurring one week after the defendant's January 13, 2022 arrest – reflect that he was informed on multiple occasions that the UAE Company 1 office in the UAE had been closed.³ For example:

Finally, as noted above, OFAC's representation that SWIFT cannot be operated out of Iran and that Iranian banks cannot utilize the SWIFT system further calls into question the legality of UAE Company 1's business activities.

³ The calls occurred in Persian. The government is relying upon translated versions of these calls, which are preliminary and subject to revision. In addition, all calls are relayed in sum and substance, and in part.

The phone calls involving the defendant's wife are not protected by the marital communications privilege both because the defendant's son was on the call and because, as is well established, calls between the defendant and his wife from jail phones are not protected by the privilege because those calls are recorded and monitored, and accordingly cannot be made with an expectation of confidentiality. See, e.g., United States v. Pugh, 162 F. Supp. 3d 97, 111 (E.D.N.Y. 2016) (NGG), aff'd, 937 F.3d 108 (2d Cir. 2019), opinion amended and superseded, 945 F.3d 9 (2d Cir. 2019), and aff'd, 945 F.3d 9 (2d Cir. 2019) (citing United States v. Madoch, 149 F.3d 596, 602 (7th Cir.1998)).

- On or about January 20, 2022, during a phone call with his son and his wife, the defendant provided directions to his wife, who then was in the physical UAE Company 1 office space, to retrieve certain items from the defendant's office. During the conversation, the defendant suggested that if the Commercial Manager⁴ was not working, an individual at Iran Company 1 who held the position of commercial director (the "Iran Company 1 Commercial Director") should hire the defendant's wife instead of the Commercial Manager. The defendant's wife responded, "I don't know! . . . they've wrapped everything up!" The defendant's wife then clarified, "they gathered and cleared-out everything in the company." In response to the defendant's inquiry as to who had done so, the defendant's wife responded that it had been the Iran Company 1 Commercial Director. She further stated that only what the Iran Company 1 Commercial Director had said could remain was still at the company, and "they took all the rest!" At various points during the conversation, she repeated sentiments to the effect, "They took it all!" In addition, at one point during the conversation, the defendant cut off discussion about locating items in his home, instead directing the focus to locating items in his office, stating, "see this is immediate now, because of this company's time is limited --."
- During the same phone call, the defendant and his wife discussed that the Commercial Manager was not working for the company. The defendant asked, "if [the Commercial Manager] isn't working – How is the company getting run?" The defendant's wife responded that she did not know.
- On or about July 23, 2022, during a call with his wife and son, the defendant asked if his secretary and others go to the company daily. The defendant's son responded, seemingly repeating his mother's statement given the quality of the call audio, "no – they emptied/evacuated the place." The defendant asked who emptied it, to which the defendant's son responded, "the people who were there."
- On or about February 4, 2022, the defendant asked his wife if she had discussed with Iran Company 1 Commercial Director being hired. After she responded no, the defendant instructed that she should ask him to hire her, and then she will go to the UAE Company 1 office. The defendant's wife asked what she would do there, to which the defendant responded, "someone has to be in that office – and you're the best choice." The defendant's wife replied, "no one works there anymore."

⁴ As set forth in Exhibit A, the Commercial Manager was an employee of UAE Company 1 from approximately 2018 until January 2020 working in UAE Company 1's physical space, and thereafter an employee of UAE Company 2. (See Plea Agreement, Ex. A ¶ 10; see also Dkt No. 31 at 5.)

The government notes that, during the end use check, Commerce also reviewed the Automated Export System (“AES”), which is a system maintained by the U.S. government in which parties must file certain information when shipping goods from the United States to a foreign country. Commerce was unable to identify any shipments to UAE Company 1, for any period. To the extent Commerce was not able to locate any shipments to UAE Company 1 even prior to the defendant’s arrest, such information likely was not entered into AES in order to conceal the illegal shipments. If so, the fact that Commerce was not able to locate records of any shipments to UAE Company 1 following the defendant’s arrest may not bear upon whether the company currently is operational.

In addition, as part of its end use check, Commerce called the known phone number for UAE Company 1. An individual answered and confirmed that he worked for UAE Company 1 and that the company was still doing business. When asked if he was available to meet to discuss U.S. exports, the individual noted that UAE Company 1 has a new email address that he could provide via a WhatsApp chat, following which the individual provided an email address associated with a domain not previously used by UAE Company 1. Law enforcement subsequently determined that the domain is registered and run out of Germany. The government respectfully submits that, based on the defendant’s jail calls with his wife described above, the fact that an individual is answering the phone at UAE Company 1 does not itself indicate that the company is continuing to operate in any meaningful – much less lawful – way. Tellingly, the defendant repeatedly suggested that his wife – who has no SWIFT or banking experience – should try to get hired at UAE Company 1, and that all she would need to do is sit in the office. The fact that UAE Company 1 apparently has a new email domain similarly does not itself indicate that the company is continuing to operate.

Finally, the government does not believe the fact that the SWIFT website continues to list UAE Company 1 itself demonstrates that the company remains operational. As the Court noted at the Sentencing Hearing, the website continues to list the defendant as the contact person for UAE Company 1. (See Tr. 29:6-8.) Given that the defendant has been in custody since January 2022, he presumably no longer is serving in that capacity, thereby suggesting that the website has not been updated. Moreover, the listed website and email address for UAE Company 1 are no longer active, further suggesting that the SWIFT website has not been updated.

B. UAE Company 2

i. Business Operations

During the Sentencing Hearing, defense counsel represented that UAE Company 1 and UAE company 2 are “completely separate companies doing completely separate things.” (See Tr. 12:23-13:1.) With respect to UAE Company 2, defense counsel stated only that it was not a SWIFT bureau. (See id. 12:23-25.) As set forth in Exhibit A, UAE Company 2 sources and procures goods and services for UAE Company 1 and Iran Company 1. (See Plea Agreement, Ex. A ¶ 11.) The government is not aware of any business conducted by UAE Company 2 other than procuring goods and services for UAE Company 1 and Iran Company 1. Indeed, the government is aware of no legitimate business conducted by UAE Company 2.

During a post-Miranda interview following his arrest, the defendant stated, in sum and substance, that the purpose of UAE Company 2 was procurement. Further, based on law enforcement's review, pursuant to judicially-authorized search warrants, of UAE Company 2's emails from approximately 2019 through 2021, law enforcement determined that all of UAE Company 2's activities during that period involved helping Iran Company 1 illegally obtain U.S.-origin goods and technology through transshipping schemes. These emails related to business and transactions (i.e., purchases of U.S. goods and technology, in violation of U.S. sanctions) between UAE Company 1, UAE Company 2, and Iran Company 1. Notably, law enforcement did not review any UAE Company 2 emails relating to business other than procuring goods for Iran Company 1. Law enforcement's review also determined that UAE Company 2 was used as an alter ego of UAE Company 1 in order to ship U.S.-origin goods and technology to Iran illegally. For example, as set forth in the Complaint, U.S. Company 3 disabled UAE Company 1's accounts because it had discovered that U.S. Company 3 software associated with UAE Company 1's license was being accessed from Iran and that one of the email addresses associated with the account belonged to an Iranian domain, and accordingly informed the Coworker that the account had been disabled because it appeared to violate U.S. export regulations. (See Dkt No. 2 ¶ 40.) The Coworker subsequently set up a new account with a U.S. Company 3 supplier using the Coworker's UAE Company 2 email address, rather than the Coworker's UAE Company 1 email address. (See *id.* ¶ 41.) The Coworker also represented that UAE Company 2 would be the end user. (See *id.*) The Coworker subsequently emailed employees at Iran Company 1 and UAE Company 2, reporting that U.S. Company 3 would not send a requested quotation because U.S. Company 3 had learned that UAE Company 2 was related to UAE Company 1, which previously had been blocked. (See *id.* ¶ 42.)

ii. Current Status

As with UAE Company 1, the government's understanding is that UAE Company 2 is no longer operational.

First, in November 2022, Commerce conducted an end use check to verify whether UAE Company 2 still is operational, as it did for UAE Company 1. As part of the end use check, Commerce reviewed the UAE Ministry of Economy's National Economic Register website, and determined that UAE Company 2's license expired in May 2022, which indicates that UAE Company 2 currently is not authorized to conduct business in the UAE. The license that expired in May 2022 was acquired by the defendant; thus, following his arrest, no one renewed or obtained a new license for UAE Company 2.

Second, UAE Company 2's email domain is no longer active. The U.S. service provider for UAE Company 2's email domain during the period of the charged conspiracy has confirmed to law enforcement that the domain is no longer registered or maintained by that provider. Similarly, UAE Company 2's website appears to have been disabled. In addition, as part of its end use check, Commerce called the known phone number for UAE Company 2, but received an automated reply that the number is not valid.

The government also notes that, as with UAE Company 1, Commerce reviewed the AES for shipments involving UAE Company 2. Commerce was able to identify only two shipments from UAE Company 2, which contained only partial information that did not fully

identify details of the shipments involved. As explained above, to the extent Commerce was able to locate very few shipments involving UAE Company 2 even prior to the defendant's arrest, the absence of recorded shipments to UAE Company 2 following the defendant's arrest may not bear upon whether the company currently is operational.

Thus, the government is not aware of any evidence that UAE Company 2 remains operational – which is not surprising given that, as set forth in Exhibit A and stipulated by the parties – the defendant was the founder, sole owner, and sole board member of UAE Company 2 (see Plea Agreement, Ex. A ¶¶ 11-13).

II. U.S. Goods and Technology

The government provides below additional information regarding the U.S. technology and goods the defendant and his co-conspirators illegally shipped to Iran, for the technology and goods specifically alleged to be part of the charged conspiracy. (See Dkt No. 2 ¶¶ 15-49.)

A. U.S. Company 1

As set forth in the Sentencing Memorandum, on behalf of Iran Company 1 and CBI, the defendant purchased from U.S. Company 1 subscriptions to a proprietary computer software program for commercial use and annual renewals for the program, as well as a digital content platform. (See Dkt No. 31 at 5.) Commerce's Bureau of Industry and Security ("BIS") has classified U.S. Company 1's software program as an information security item subject to national security and anti-terrorism controls, pursuant to Export Control Classification Number ("ECCN") 5A002.a.

The U.S. Company 1 software program is sophisticated development software that enables large organizations to develop proprietary online and/or mobile applications, and then to deploy those applications directly to their employees on secure internal company systems or through company mobile devices. For example, a bank could use the software to create a secure online application, such as a mobile banking application, that the bank employees could use on their computers and/or cell phones, in order to quickly and securely move funds. The U.S. Company 1 digital content platform is an application that enables the quick transfer of files between electronic devices. For example, a bank employee could use the digital content platform to transfer financial transaction data between computers or company mobile devices much faster than the employee could using wireless internet or Bluetooth capability.

Here, the defendant provided the U.S. Company 1 development software program and digital content platform to Iran Company 1 and CBI, presumably enabling them to utilize the U.S. Company 1 software to conduct their operations more efficiently, effectively, and securely. As set forth in Exhibit A, Iran Company 1 is the largest electronic banking organization in the Middle East and provides information technology services to almost all Iranian commercial banks and many Iranian financial institutions. (See Plea Agreement, Ex. A ¶ 17.) U.S. Company 1's development software and digital content platform presumably facilitated Iran Company 1's ability to conduct these operations, including for services it provides to CBI. With respect to CBI, providing this technology likely not only enabled the Iranian banking system to operate more

effectively, but helped to further CBI's agenda of materially assisting, sponsoring and providing financial, material or technological support, goods or services to Lebanese Hizballah, a terrorist organization, and to the Qods Force of Iran's Islamic Revolutionary Guards Corps, a branch of the Iranian armed forces and the Iranian government's primary means of directing and implementing its global terrorism campaign (see Dkt No. 2 ¶ 4; Dkt No. 31 at 4). Although the government is not able to determine the specific purposes for which Iran Company 1 and CBI use the U.S. Company 1 software and digital content platform, and accordingly cannot evaluate the specific effect of the defendant's conduct in providing this technology, the government notes that CBI itself considered its access to the software to be important. As set forth in the Complaint, in 2020, a CBI employee requested "immediate renewal" and emphasized the importance of the task given the limited time before the program expired, recognizing that purchasing a new subscription would be practically impossible due to sanctions. (See Dkt No. 2 ¶ 20.) Indeed, the defendant purchased subscriptions and annual renewals for the program from 2016 through 2021, itself suggesting that the program was of significant value to Iran Company 1 and CBI. (See id. ¶¶ 16-21.)

B. U.S. Company 3

As set forth in the Sentencing Memorandum, on behalf of Iran Company 1, the Coworker purchased renewals for two subscriptions to U.S. Company 3's operating system. (See Dkt No. 31 at 6.) U.S. Company 3's operating system is the world's leading enterprise Linux platform, which is an open-source operating system. As an open-source operating system, a company can access the operating system, which manages hardware and software (including cloud-based software), and modify the operating system for the company's specific needs. For example, a bank can use Linux operating system software to provide technological services needed to operate the bank, including with respect to conducting financial transactions with other banks.

Here, the defendant and his co-conspirators provided the U.S. Company 3 operating system software to Iran Company 1, presumably enabling Iran Company 1 to utilize the U.S. Company 3 software to conduct its operations – including with respect to facilitating the Iranian banking system – more efficiently, effectively, and securely. As with the U.S. Company 1 software, the government is not able to evaluate the specific effect of the defendant's and his co-conspirators' conduct in providing the U.S. Company 3 software. However, a confidential informant who previously worked at Iran Company 1 has advised law enforcement that U.S. Company 3's operating system software is highly desired, and has been used by Iran Company 1. In addition, as with the U.S. Company 1 software, Iran Company 1 itself seemingly considered the U.S. Company 3 software to be of considerable value. Iran Company 1 used the software for approximately five years, itself suggesting the value of the operating system software to Iran Company 1. And, tellingly, when U.S. Company 3 disabled UAE Company 1's access because the software was being used in Iran in violation of U.S. sanctions, the defendant's co-conspirator tried to procure access to the U.S. Company 3 operating system software under UAE Company 2's name. (See Dkt No. 2 ¶¶ 40-42.) The co-conspirator's effort to create a new account in UAE Company 2's name in order to access the U.S. Company 3 software further demonstrates that program's value to Iran Company 1.

C. U.S. Company 2

As set forth in the Sentencing Memorandum, on behalf of Iran Company 1, the Coworker purchased “fixed attenuators,” which are devices found in various electronic equipment with uses including extending the range of certain equipment and preventing signal overload in transmitters and receivers, from U.S. Company 2. (See Dkt No. 31 at 6-7.) Broadly, an attenuator is an electric device that reduces the power of a signal, thereby reducing the electrical/electronic energy passing through a device, without degrading the integrity of the device. For example, a fixed attenuator can be used in a bank’s computer systems to lower the voltage (i.e., internet traffic) in order to prevent the system from overloading and shutting down (thereby temporarily causing loss of access to the bank’s money) when a large number of people are using the system at the same time. Although fixed attenuators generally are inexpensive devices, they play an essential role in ensuring the functionality of large electronic devices and systems.

Here, the defendant and his co-conspirators provided the U.S. Company 3 fixed attenuators to Iran Company 1, presumably enabling Iran Company 1’s computer systems to avoid overloading and shutting down. As set forth above and in Exhibit A, Iran Company 1 is the largest electronic banking organization in the Middle East, provides information technology services to almost all Iranian commercial banks and many Iranian financial institutions, and has hundreds or more employees. (See Plea Agreement, Ex. A ¶ 17.) Given its size and the scale and nature of its operations, U.S. Company 2’s fixed attenuators likely play a critical role in ensuring the functionality of Iran Company 1’s computer systems, thereby broadly facilitating Iranian banking.

D. U.S. Company 4

As set forth in the Sentencing Memorandum, on behalf of Iran Company 1, the Coworker purchased network storage systems and six power supplies from U.S. Company 4. (See Dkt No. 31 at 7.) Specifically, the Coworker purchased enterprise storage systems designed for storage area network environments and power supply systems that support the storage systems. BIS has classified U.S. Company 4’s network storage systems and power supplies as information security items subject to national security and anti-terrorism controls, pursuant to ECCN 5A002.a.

The U.S. Company 4 storage systems – touted for their unprecedented performance, functionality, and cost efficiency – enable large-volume data processing and cloud storage, which, among other things, facilitates easily organizing and locating files notwithstanding the significant quantity of stored data. For example, banks – which rely upon massive data and large electronic systems to maintain, transfer, and manipulate monetary transactions – can use the U.S. Company 4 storage systems to maintain, store, and organize their infrastructure. The power supply systems provide power to these network storage systems.

Here, the defendant and his co-conspirators provided U.S. Company 4’s enterprise storage systems and power supplies to Iran Company 1, presumably enabling Iran Company 1 to conduct its operations more efficiently, effectively, and securely. As the largest electronic banking organization in the Middle East and in its capacity as providing information technology services to almost all Iranian commercial banks and many Iranian financial institutions (see Plea Agreement, Ex. A ¶ 17), Iran Company 1 presumably requires enormous electronic storage

capabilities and power to operate. U.S. Company 4's enterprise storage system and power supplies likely helped it to do so.

III. Effects of the Illegal Transshipping Scheme

As set forth in the Sentencing Memorandum, the Executive Branch has determined, as a matter of foreign policy and U.S. national security, that the threat posed by the Government of Iran – a country that sponsors international terrorism – is so severe that only sanctions and a trade embargo on certain U.S.-origin goods, technology, and services are adequate to protect the interests of the United States. (See Dkt No. 31 at 15.) That determination is within the sound judgment of the Executive Branch. (See *id.*) And, notably, in 2020, OFAC identified the Iranian financial sector as subject to Executive Order 13902, which authorized sanctions intended to deny the Iranian government revenues that could be used to fund and support its nuclear program, missile development, terrorism and terrorist proxy networks, and malign regional influence.

Here, the defendant and his co-conspirators illegally provided Iran Company 1 and CBI – an agency of the Government of Iran – with sophisticated, top-tier U.S. electronic equipment and software that enabled the Iranian banking system to operate more efficiently, effectively, and securely. In doing so, the defendant and his co-conspirators likely helped strengthen Iran's economy and provided faster and more secure access to funds that enable the Government of Iran to further priorities including its nuclear program and terrorist agenda. That is exactly what the U.S. sanctions against Iran were intended to prevent. Tellingly, a confidential source who previously worked for Iran Company 1 informed law enforcement that Iran Company 1 and the broader Iranian banking system rely on U.S. software to operate, including technology from some of the most sophisticated U.S. technology companies. The source further has advised that, historically, Iran Company 1 had outdated banking systems and software. That likely is why Iran Company 1 tasked the defendant with procuring advanced U.S. software and electronic goods – to improve Iran Company 1's, as well as CBI's, functionality, and in turn, the operations of the broader Iranian banking network. The defendant's conduct thus not only undermined U.S. sanctions against Iran and the Executive Branch's repeated declarations that the actions of the Government of Iran are a threat to national security, but helped the Iranian banking system to operate. That is not merely a technical sanctions violation, but a serious national security breach.

IV. Forfeiture

During the Sentencing Hearing, the Court inquired why the government had not sought forfeiture of the defendant's interests in UAE Company 1 and UAE Company 2. (See Tr. 31:16-24.) The government did not seek forfeiture as part of the plea agreement because of the logistical complexity of forfeiting the defendant's interest in the two internationally-based front companies and because of the government's understanding that the companies are no longer operational. However, the defendant's interests in UAE Company 1 and UAE Company 2 are one of the reasons that the government required a \$50,000 fine as part of the plea agreement. (See Plea Agreement ¶ 7.)

The government notes also that it has notified the UAE government, via the Financial Crimes Enforcement Network, of the illegal activities by the defendant, UAE Company

1, and UAE Company 2. The government takes no position on what, if any, action the UAE government may take with respect to UAE Company 1 and/or UAE Company 2.

V. Conclusion

The government respectfully submits that the information above supports its position, set forth in the Sentencing Memorandum and during the Sentencing Hearing, that the calculation of the defendant's offense level should include a four-level enhancement pursuant to U.S.S.G. § 3B1.1(a), such that the defendant's adjusted offense level is 27 and the Guidelines range of imprisonment is 70-87 months. The government further submits that, given the serious nature of the criminal conspiracy and the defendant's role in that conspiracy – and the threat to U.S. national security posed by the actions of the defendant and his co-conspirators – a sentence within the Guidelines range is appropriate.

Respectfully submitted,

BREON PEACE
United States Attorney

By: /s/
Alexander A. Solomon
Meredith A. Arfa
Assistant U.S. Attorneys
(718) 254-7000

Cc: Clerk of the Court (by ECF and Email)
Babak Hoghooghi, Esq. (by ECF)
William F. Coffield, Esq. (by ECF)